Chapter 1: The Windows 2000 Environment at Fermilab

In this chapter we introduce you to the environment at Fermilab for networked Windows systems, namely the Windows 2000 strengthened domain, FERMI.WIN.FNAL.GOV.

1.1 Introduction to Windows 2000

Windows 2000 (W2K) is one of the family of Windows operating systems from Microsoft, the successor to NT4. Its user interface is similar to that for Windows NT/95/98, and works in much the same way as other Windows systems you may already be familiar with.

Computers that run Windows can be configured as stand-alone, as part of a work group, or as members of a domain. Work groups and domains are groupings of computers, typically set up for resource-sharing.

The W2K operating system was designed primarily for use in multi-server networks and strengthened domains. A strengthened domain is a set of networked desktops, servers and other computing resources that are identified to a central controller as requiring strong authentication[1] for access from the network. The central controller defines the domain and grants authentication requests. Kerberos is the default strong authentication protocol used.

In plain English: From your networked W2K desktop,

- You type in a Kerberos password to identify yourself.
- A message gets sent over the network so that the domain controller knows that you are really who you say you are.
- Then you can use the domain's networked printers, file servers, and so on, to your heart's content.

1. Strong authentication and Kerberos are described in the *Strong Authentication at Fermilab* manual. See `http://www.fnal.gov/docs/strong-auth/`.

1.2 The Windows 2000 FERMI Domain

At Fermilab, the Computing Division has built a strengthened Windows 2000 domain called FERMI.WIN.FNAL.GOV, or FERMI for short. As of early 2003, a limited number of Windows-based resources (e.g., disk shares and printers) are already in the FERMI domain. In coming months, many more will be added.

All domain users must possess a FERMI domain Kerberos principal and password (see section 2.2 *Kerberos Principals and Primary Accounts*). Note that CRYPTOCards[1] cannot be used for authenticating to the FERMI domain.

We discuss requirements and recommendations for joining the FERMI domain in section 1.4 *The FERMI Domain and your Computer* and in Chapter 2: *Joining the FERMI Domain*.

1.3 What are the Advantages of the FERMI Domain?

The FERMI domain provides several advantages, both for users and administrators:

- Central management of user accounts. Instead of creating individual user accounts on each computer a user needs, domains use a common database of user accounts.
- Central management and unification of security policies that help protect your computer from attacks, and that meet DOE and FNAL requirements.
- Central management of resources. Domains allow server administrators the ability to centralize the management of disk and printer resources. Users can locate these resources easily.
- Central management of desktop updates. Computers in the domain can receive security information and software updates from a common support group.
- Grouping of users into Organizational Units (OUs), based upon the organization (experiment, division, department) with which they are affiliated. Many of the administrative decisions and tasks are handled at the OU level, rather than at the (higher) domain level.

1. CRYPTOCards are described in the *Strong Authentication at Fermilab* manual; see `http://www.fnal.gov/docs/strongauth/get-start.html`.

- Options for tuning a user's roaming profile for better performance (see section A.4 *User Profiles in the FERMI Domain*).

As an end user of the W2K FERMI domain, you have access to a variety of computing resources and services, for example:

- File storage, backup, virus-checking and disaster recovery (see Chapter 5: *File Management*).
- Virus-checked software as well as Computing Division-supported software patches (security, OS, workstation), and updates for applications and device drivers.
- Wide variety of printers at the lab, through various servers (see the *Printing* Web page for information on printing).

1.4 The FERMI Domain and your Computer

1.4.1 Permanent/Long-term On-site Systems

The Computing Division recommends that all long-term on-site Windows 2000 or XP (Professional, not the home edition) systems be configured as members of the FERMI domain. Other Windows operating systems are not supported by the domain, but they may still be configured to access domain resources (see Chapter 4: *Authenticating and Accessing Domain Resources from Non-Domain Machines*).

1.4.2 Remote Systems

For systems that remain predominantly or always off-site, we recommend that they do not get placed in the FERMI domain. Fermilab blocks the various NetBIOS ports to the FERMI domain controllers, which prevents off-site systems from logging into the domain (although off-site users may be able to access particular domain resources using cached credentials; see section 2.4 *Off-site Use*). Only computers that are physically attached to the on-site Fermilab network will be able to log into the domain. In addition, Fermilab has no control over what network blocks an ISP may enforce on its portion of the network.

If you want to place your off-site system in the domain, your OU manager has the authority to evaluate your situation and decide whether to allow your remote system to join the FERMI domain. See section 7.1 *General Windows Support Information*.

1.4.3 Short-term/Visiting On-site Systems

For short-term visitors and contractors, typically it is not practical to place your computer in the domain. A set of security policies and software gets deployed on computers that join. Some of the FERMI settings might prevent your computer from functioning properly once you return to your home institution. However, if you connect to the Fermilab network, you must make sure that your computer is protected from the attacks that occur routinely on the internet. If your machine gets hacked, you will likely be contacted by Fermilab computer security.

To protect your computer, please take the following steps:

- Run Windows Update and make sure your machine has the latest security patches
- Install and configure anti-virus software so that it scans files in realtime and updates virus signatures daily
- Disable file/print sharing services
- Configure Kerberos or NTLMv2 authentication, if possible (although this may cause problems back at your home institution)
- If you need to connect to remote UNIX hosts at Fermilab, install software that allows you to make Kerberized connections, e.g., WRQ® Reflection (see section 6.1 *Connecting to Remote UNIX Hosts*).

Another option to consider is to connect to a Windows Terminal Server. Please consult with your Fermilab computer liaison for information about this and to see if it would work for you.

1.5 Authentication and Accessing Resources

Domain Computers

If your system has been added to the FERMI domain, you will log directly into the FERMI domain when you log into your computer. This will require entry of your (FERMI) Kerberos password, and you'll be automatically authenticated via Kerberos to the domain. For the present this means that you'll have access to resources in both your old NT4 domain and the W2K FERMI domain. You should notice no interruption or difference as resources move from the NT4 FNAL domain to FERMI.

Once your machine is added to the FERMI domain, never attempt to log into your machine using your NT4 (i.e., FNAL domain) account and password. In other words, don't use your FERMI domain machine to log into an NT4 domain.

Also, if you still have access to computers that are resources in the older NT4 domains, DO NOT use your FERMI domain account and password to log into those machines.

Non-Domain Computers

If your computer is not a member of the domain, you will need to log into that computer using your local account/password. If you only require access to resources in the NT4 domain, you will not need to take any further action. If you require access to resources in the FERMI domain, you will need to upgrade your computer so that it can use NTLMv2 authentication. We provide more information on NTLMv2 in `Chapter 4:` *Authenticating and Accessing Domain Resources from Non-Domain Machines.*